International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Trusted and Protection of Exemplary Eventualities of Threats against Privileged Data Secrets across Sleepwake Cycles in Personal Computers

K.Tulasi, Ch.Anand Krishna, M.D.Ajay Sachin, Dr.K.V.D.Kiran, Venkata Naresh Mandhala

Abstract*: Our paper notices that with a high probability the computer faced with physical attacks can be in a suspended mode. We have more interest in addressing a series of existing and plausible threats to cyber security where the opponent possesses unconventional attack capabilities. Such unconventionality includes, in our exploration t but not restricted to, crowd sourcing, physical coercion, substantial machine resources, malicious insiders, etc. Throughout this paper, we have a tendency to tend to demonstrate but our philosophy is applied to affect several exemplary eventualities of unconventional threats, and elaborate on the model systems data secrets across sleepwake cycles. Most PCs, particularly laptops, remain in rest suspend to RAM, when not in dynamic use. A vital inspect for unattended PCs in rest is that the nearness of client insider facts in framework memory. An aggressor with material approach of a computer in rest will launch side vein memory attacks, by handling liable device drivers; regular mitigations include like bugs etc. A sophisticated assailant can likewise fall back on chilly boot assaults by handling DRAM memory impact. Hypnoguard2 protects in RAM information once a laptop is in sleep simply just in case of assorted memory attacks ecosystem for every desktop and mobile platforms, the appliance of reliable computing still remains rare or exclusively by certain manufacturers. In reality, a way larger issue is that the inspiration of trust is sometimes a combination, this becomes a significant barrier for the tutorial analysis due to lack of access to hardware primitives or public documentation. We believe the high level methodology of these research topics can contribute to advancing the security research under strong adversarial assumptions, and the promotion of software hardware orchestration in protecting execution integrity therein.

Manuscript published on November 30, 2019.
* Correspondence Author
K.Tulasi*, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: 160030698@kluniversity.in
Ch.Anand Krishna, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: 160030227@kluniversity.in
M.D.Ajay Sachin, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: 160030816 @kluniversity.in
Dr.K.V.D.Kiran, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: kiran_ces@kluniversity.in
Venkata Naresh Mandhala, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. Email: mvnaresh.mca@gmail.com

***Keywords*: protection, eventualities, threat, data, pattern, Hypnoguard2.**

I. INTRODUCTION

In this paper, we have a tendency to explore approaches to such security issues underneath a powerful adversarial model. Within the domain of authentication and knowledge protection (e.g.,for integrity and confidentiality The initial known crypto ransomware dates back to only directory names were encrypted. Crypto based attack vectors were formally introduced by Young and Yung in 1996. when the Crypto Locker attack in 2013, strong crypto ransomware families are growing steady, with an outsized range of attacks. A vital inspect for unattended PCs in rest is that the nearness of client insider facts in framework memory. Safeguarding just cryptographic keys likewise seems, by all accounts, to be fundamentally faulty, additional security delicate contentment in RAM. Full memory cryptography is accustomed keep all RAM content scrambled, as used in recommendations for encoded execution [1]. Be that as it may, most such recommendations need equipment field changes. This presents observable deferrals inside the rest wake technique. More significantly, Bit Locker isn't designed to face up to coercion and may offer solely restricted defense against watchword idea attacks. We tend to propose Hypnoguard2 to guard all memory resident user knowledge across sleep wake suspensions, against memory extraction assaults, and speculating of client passwords all through wake up time reauthentication Memory extraction is relieved by performing arts Associate in Nursing set up full memory cryptography before getting into rest, at that point reestablishing the plaintext privileged insights once the wakeup technique[2].The memory cryptography secret's encrypted by a Hypnoguard2 public key, personal a part of that will keep in very sure Platform Module (TPM) chip, ensured by each the client watchword and thusly the proportion of the execution setting upheld by CPU's certain execution mode, e.g.,Intel sure Execution innovation and AMD Virtualization. The memory cryptography secret's so guaranteed to the execution setting, and may be discharged solely by a correct reauthentication method.

Guess via Hypnoguard2 could cause the memory substance to be for good difficult to reach thanks to the erasure of the TPM put away Hypno guard2 personal key, e.g., Associate in Nursing aggressor picked custom wakeup technique is looking like savage compelling a high entropy key, on account of TPM security. A user defined policy, e.g., 3 unsuccessful makes an attempt, or a special deletion watch word, determines once the personal\secret's deleted. Thus, either the personal key can't be accessed thanks to associate in Nursing incorrect measure of Associate in Nursing changed program, or the human goes out on a limb to figure inside the unmodified setting. Due to the eccentricity of the wake up time air, we will in general face numerous difficulties in actualizing Hypnoguard2. Not at all like boot time (when peripherals square measure initialized measure instated by BIOS) or runtime (when gadget drivers inside the OS square measure dynamic), at wake up time, the framework is left in partner dubious state, e.g., void PCI setup zone and uninitialized I/O controllers. We tend to style the goal of hyperguard2 custom drivers and recycle dormant Operating system spared gadget setups to restore the console and VGA show to encourage basic client yield. We style Hypnoguard2 a substitution approach that secures secrecy of all memory locales containing OS data crosswise over rest wake cycles. We offer a guard against memory assaults once the pc is inside an inappropriate hands, and seriously disallow thought of feeble verification mysteries ,Several proposition and apparatuses exist to shield information very still (e.g., plate stockpiling), information in travel (e.g., organize traffic), and information in use (e.g.,live RAM content) ;with Hypnoguard2, we will in general fill the hole of verifying information in rest. Our essential picture usage in Linux utilizes full memory coding to evade per application changes. The center a piece of Hypnoguard is decoupled from the fundamental OS and framework BIOS, for higher mobility and security [4].

A. Goals:

We preponderantly believe assaults focusing on extraction of insider facts through physical access from a compact PC in rest[7]. We would wish to safeguard memory resident secrets against side channel attacks, but we've got an inclination to do not consider compromising a computer in sleep.

1) Any user or software system package info mustn't keep in plaintext anyplace in RAM before continuing the software system package to create memory attacks orthogonal.

2) The protected content mustn't be retrieved by brute – forcing, even supposing Hypnoguard2 isn't dynamic, e.g., by means of online assaults.

3) No dead reckoning attacks have to be compelled to be accomplishable against the Hypnoguard2 user word, except if a genuine duplicate of Hypnoguard2 is stacked because of the alone program in execution [8].

4) The legitimate user has to be compelled to be able to demonstrate with routine exertion, e.g., memorization of solid passwords isn't required.

5) Theory the client word once Hypnoguard2 is dynamic must be constrained to be seriously confined by the punishment of getting the privileged insights erased..

II. PROPOSED SYSTEM

Hypnoguard2: Safeguarding secrets across sleepwake cycles

Aggressors can get physical administration of a workstation in rest in the event that it lost, taken, or the proprietor is stressing. High esteem memory occupant privileged insights, furthermore as disk secret writing keys, and private encryption keys, is expansion partner removed by physically getting to a PC. We will likely ease dangers of removing privileged insights from a PC in rest[5], whereas not wishing on web confronting administration. we will in general propose Hypnoguard2 to ensure all memory resident user information, by first activity Associate in Nursing in place full memory secret writing before coming back into sleep, at that point reestablishing the plaintext content at wake up time through condition bound, secret key based confirmation technique. The memory secret writing key's effectively "sealed" in an exceedingly very trustworthy Platform Module chip with the measurement t of the execution atmosphere supported by the CPU's trustworthy execution mode. Secret shot via Hypnoguard2 would possibly cause the memory substance to be permanently out of reach because of the cancellation of the dependable Platform Module stored Hypnoguard2 personal key, whereas shot whereas not Hypnoguard2 is like brute forcing a high entropy key[6]. To our data Hypnoguard2 gives the first wake up time secure environment for authentication also, key opening, while not requiring per application changes.

III. PROCEDURE

1. A methodology that secures classification of all memory districts containing client data crosswise over rest wake up cycles. we give resistance against memory assaults once the PC is at interims the mistaken hands, and seriously interdict gauge of powerless validation privileged insights.

2. Our primary model implementation in any software system uses full memory cryptography to avoid per application changes. The core a locality of Hypnoguard2 is decoupled from the underlying code for higher movableness and security.[9].

IV. TERMINOLOGIES

A. Hypnoguard2key combine(HGpub, HGpriv ,HGHyd):

A blend of open and private keys created all through arrangement. HGpriv is recovered through the counter sign assessed by TPM with the Hypnoguard2 program running, and could be for all time erased as per a client set arrangement. the general open key, HG bar is stacked in RAM once each boot and HGhyd is taken consideration concerning remaining choices.

B. Hypnoguard2 user password:

A client picked slogan to open the ensured key HGpriv at wake up time. It's to set about to entirely a handful of guesses, betting on the actual unlocking policy.

Retrieval Number: D5397118419/2019©BEIESP
DOI:10.35940/ijrte.D5397.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

C. TPM "sealing":

For safeguarding HGpriv in trustworthy Platform Module, we have a tendency to use the Define Space command, that provides atmosphere binding and authentication data (password) protection.

D. Memory cryptography key:

A high entropy interchangeable key, haphazardly generated on each occasion before returning into rest, and utilized for full memory cryptography. Before the framework enters rest, secret's encrypted practice HGpub and conjointly the following ciph er text is hold on at intervals the small nonencrypted region of memory. Traces elsewhere left by the data to be erased are out of scope are going to be identified by HGhyd.[12].

V. DESIGN

User secrets square measure created unprocurable from RAM by encoding the entire framework memory, notwithstanding bit or client territories, with a onetime arbitrary symmetric key (SK) before going in rest. At that point symmetric mystery is encoded exploitation public key of Hypnoguard2 and detain system memory. At now, alone personal key of hypnoguard2 can rewrite symmetric key(SK).Personal key of Hypnoguard2 is sealed among the positive platform module(TPM) chip with the measurements of Hypnoguard2 protected by a user watchword. At wakeup time, Hypnoguard2 takes management terribly} very positive execution session, and prompts the user for the Hypnoguard2 user watchword, provided that the correct watchword is provided at intervals the important Hypnoguard2 atmosphere, personal key of Hypnoguard2 is unsecured from TPM.[13]

A. Trusted execution mode:

We execute the opening system at interims the specific method of most recent CPUs, where Associate in Nursing unforgettable activity of the execution surroundings is created and hang on in TPM. the use of TPM guarantees that the total program being stacked and dead area unit reflected at intervals the activity. We decide to remain Hypnoguard2 as a standalone module become independent from the package for two reasons

1. Small trusted computing base:

In the event that Hypnoguard2's opening project is incorporated with the OS, at that point we have a tendency to tend to ought to conjointly embody OS elements inside the TPM live. Also, terribly} very shopper OS, keeping up the best possible estimations of such somewhat dedicated figuring crosswise over continuous updates and runtime changes, are irksome. Except if estimating the whole OS is that the point secured application is typic partner a piece bit of code, not incorporated with the bundle, to fathom a steady and manageable faithful registering base.[10]

2. Portability:

We create Hypnoguard2 less not to mention the hosting OS aside from simply a kernel driver, as we have a tendency to might have to figure with totally different distributions of associate degree software system.[11]

B. TPM'S Role:

TPM serves three functionsinHypnoguard2:

1)By operative with reliable Execution Technology(TXT) reliable Platform module(TPM) configuration registers maintain the unforgeable activity of the execution setting.

2) We shield nonpublic key of Hypnoguard2 by storing safely with 2 layers of protection. First, nonpublic key of Hypnoguard2 is certain to the Hypnoguard2 setting. Any binary apart from real copy of hypnouard can fail to access nonpublic key of Hypnoguard2.Second, a licensed knowledge secret, derived from the Hypnoguard2 user password, is additionally accustomed shield nonpublickeyofHypnoguard2.

3) If nonpublic key of Hypnoguard2 is deleted by the Hypnoguard2, we tend to conjointly give a trusty platform module quote that could be a digest of the platform activity.

C. How Goals are achieved:

Goal one is consummated by Hypnoguard2's full memory secret writing, i.e., of all plaintext memory content, with comparing figure content produced by key. Because of the usable frameworks or applications are not engaged with place memory secret writing are usually performed reliably. Encoding key resides in memory encrypted below public key of Hypnoguard2. Personal key of Hypnoguard2 can alone be unsecured with the right environment and recognizable proof at wakeup time, and is eradicated from RAM right once its utilization inside the specific execution mode. A irregular encoding key with sufficient length created whenever before getting in rest, and a solid open key attempt(HGpub, HGpriv, HGhyd) generated all through setup ensure Goal two. TPM protection helps deliver the products Goal three. The human is to boot incapable to beast power the apparently feeble client distinguishing proof, on the off chance that he is happy to program the TPM chip while not Hypnoguard2, as TPM guarantees the steady disappointment message for each erroneous passwords and inaccurate estimations. The client is required to check AN everyday identification for authentication. If the human keeps the surroundings but does not acknowledge the correct identification, he's additionally alone left with a high danger of erasing HGpriv. The authentic client, in any case, is tuned in to the identification and should management the prospect of accidental deletion e.g., via setting degree applicable deletion threshold Therefore Goal four is glad. When the human guesses among Hypnoguard2, the identification theme makes positive that no guess tries unit permitted before erasure is activated. This achieves Goal five.

VI. IMPLEMENTATION

We discuss our implementation of Hypnoguard2 underneath UNIX operating system victimization Intel TXT because the trusty execution supplier. Note that Hyp noguard2's style is OS freelance, however our current implementation is UNIX operating system specific, the sole part that has got to be developed for various OS es is Hypno OS Service.

we've an inclination to together performed AN experimental analysis of Hypnoguard2's user experience no noticeable latency was discovered at wake up time.[14]

The Hypnoguard2 tool consists of three parts:

- HypnoCore(the unlocking rationale and figure motor),
- HypnoDrivers (gadget drivers use data wakeup time),and
- HypnoOSService(part administration to rework for HypnoCore).

HypnoCore and HypnoDrivers work outside of the PC code, and HypnoOSService runs at interims the PC code.

EXECUTION STEPS:

a) The planning is finished by Hypno OSService whenever while the OS is running before activated. HypnoCore, HypnoDrivers, ACM module for TXT, and conjointly the TXT approach document square measure derived into mounted memory locations celebrated by Hypnoguard2 . Likewise, Hypno OS Service registers itself to the OS portion so as that if the client or a framework administration starts Sleep wake, it's conjured.

b) Upon passage, essential parameters for TXT square measure arranged and keep, and conjointly the part's memory tables square measure supplanted with our own, map ped for Hypno Core and Hypno Drivers.[21,22].

c)Then, Hypno Core encodes the total memory in an exceedingly in no time manner through multi core method with AES CTR mode pattern symmetric key. Before triggering the actual S3 action by inflicting commands, Hypnoguard2 ought to supplant the underlying OS waking vector to instigate the executives back once the machine is arouse up.

d) At wakeup, the 16piece genuine mode section, dwelling beneath 1MB of Hypnoguard2 waking vector is activated. It calls HypnoDrivers to reintroduce the console and appear, and plans TXT memory structures and page tables.

e) At that point the client is incited for a mystery, that is used to open TPM NVRAM records individually. Upheld the result and conjointly the specific opening strategy, either erasure of HGpriv happens instantly and a statement is generated for additional confirmation, or if the key is right, HG priv is unfastened into memory. Once decrypting symmetric key, HGpriv is deleted instantly from memory. Hypno Core at that point utilizes key to translate the total memory.

A typical constraint of those arrangements is that particular cryptographical activities ought to be stacked from the protected application to the new instrument, commanding per application changes. They're conjointly targeted on preventing escape of solely crypto graphical keys, that is essentially restricted in protective RAM content normally

Also, some solutions don't contemplate user reauthentication at wake up time. many of them determine their lord mystery, or its proportionate, from the client parole, this may even allow the human to legitimately figure the ace mystery in partner degree online way[19].Memory secret writing A perfect resolution for memory extraction assaults is perform scrambled execution: headings stay encoded in RAM partner degreed territory unit decoded directly before execution at interims the CPU; see XOM for an early proposition during this space, and Henson and Taylor for a thorough overview. Most proposition for memory secret writing manage information in use by an energetic processor. Our utilization of full memory mystery composing includes the rest state, when the processor is basically idle.[20]

Most frameworks need bailiwick changes in equipment and in this way remain generally un adopted, or intended for specific use cases, e.g., bank ATMs. Misuse committed custom processors, some diversion supports conjointly actualize memory mystery keeping in touch with some degree[23].

VII. CONCLUSION

As most PCs, particularly, workstations, keep in rest while not effectively utilized, we have a bowed to contemplate an exhaustive rundown of dangers against memory occupant client OS data, security touchy. we have a twisted to manage a significant hole left in existing arrangements: far reaching secrecy insurance for information in rest, when the attacker has physical access to a Workstation rest. we have sent to vogue and actualize Hypnoguard2, that scrambles the whole memory rapidly before returning into rest beneath a key fixed in sure stage module with the respectability of the execution air. we have a twisted to need no per application changes or piece patches. Hypnoguard2 upholds client re validation for opening the key at wake up time during a very TXT empowered solid air. Plan assaults bypassing Hypnoguard2 are rendered inadequate by the properties of reliable platform module waterproofing, and plan within Hypnoguard2 will trigger erasure of the key. In this way, Hypnoguard2 next to a boot time insurance system with Full disk secret writing support can amendment effective serverless plan resistance, once a laptop computer with sensitive info is lost or taken. Most present verification

plans would neglect to relate somebody UN office is eager to utilize human encourage to hinder into existing systems that are intended to restrain exclusively machine driven assaults. As client accounts generally become extra and extra significant with the length of utilization, it will be commendable for aggressors to guess in minimal effort human work as a method to bargain client accreditations. In thinking of Hyperguard, we tend to explicitly consider such dangers and supply limited assurance.

VIII. FUTURE SCOPE

In a broader sense, it is like a privilege race, e.g., a hypervisor level mechanism should be effective against guest kernel level threats and so forth. Therefore, undoubtedly hardware can attain the lowest protection level (highest privilege) in the battle with various adversaries. Existing hardware enforced mechanisms still have room for improvements in the following aspects like Trust anchor. In trusted computing, the first link of the trust chain is usually an immutable and protected secret that binds to the hardware (the place storing the unique secrets, which is called Secure Element in certain terminology).

Retrieval Number: D5397118419/2019©BEIESP
DOI:10.35940/ijrte.D5397.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

REFERENCES

1. D. Abramson, J. Jackson, S. Muthrasanallur, G. Neiger, G. Regnier, R. Sankaran, I. Schoinas, R. Uhlig, B. Vembu, and J. Wiegert. Intel virtualization technology for directed i/o. Intel technology journal, 10(3), 2018.
2. M. Alsaleh, M. Mannan, and P. van Oorschot. Revisiting defenses against largescale online password guessing attacks. IEEE Transactions on Dependable and Secure Computing (TDSC), 9(1):128141, 2018
3. Lianying Zhao ,Authentication and Data Protection under Strong Adversarial Model, IEEE Transactions on Dependable and Secure Computing (TDSC), 9(1):128141, 2018
4. A. Filyanov, J. M. McCuney, A.R. Sadeghiz, and M. Winandy. Unidirectional trusted path: Transaction confirmation on just one device. In IEEE/IFIP Dependable Systems and Networks (DSN'11), Hong Kong, June 2017.
5. R. A. Fink, A. T. Sherman, A. O. Mitchell, and D. C. Challener. Catching the cuckoo: Verifying tpm proximity using a quote timing sidechannel. In J. M. McCune, B. Balache, A. Perrig, A.R. Sadeghi, A. Sasse, and Y. Beres, editors, Trust and Trustworthy Computing, pages 294301, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.
6. B. A. Fisch, D. Vinayagamurthy, D. Boneh, and S. Gorbunov. Iron: Functional encryption using intel sgx. 2016.
7. Prakash, K.B. & Rangaswamy, M.A.D. 2016, "Content extraction of biological datasets using soft computing techniques", Journal of Medical Imaging and Health Informatics, vol. 6, no. 4, pp. 932-936.
8. K.V.D.KIRAN," "Literature Review on RisK Literature Review on Risk and their Components" International Journal for Research in Emerging Science and Technology (IJREST) ",Volume1, Issue6, November 2014", (eISSN 23497610).
9. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE TIFS, 8(1):136148, Jan. 2014.
10. K.V.D.KIRAN,"Integrated Distributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare," International Journal of BioScience and BioTechnology", Vol.7, No.3 (2015), pp.243250, ISSN: 22337849 IJBSBT.
11. M. Frank, T. Hwu, S. Jain, R. Knight, I. Martinovic, P. Mittal, D. Perito, and D. Song. Subliminal probing for private information via EEGbased BCI devices. Techreport (Dec. 20, 2013)
12. J. Götzfried and T. Müller. Mutual authentication and trust bootstrapping towards secure disk encryption. ACM Transactions on Information and System Security (TISSEC), 17(2):6:16:23, 2014
13. K.V.D.KIRAN,"A Critical study of information security risk assessment using fuzzy and entropy methodologies," International Journal on Computers and Communications", Pages: 1722,Vol1,Isuue1,Dec,12, ISSN: 2319 – 8869.
14. K.V.D.KIRAN,"Performance Analysisof Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm", IEEE CS'07, SIVAKASI, TAMIL NADU,India
15. K.V.D.KIRAN," MULTI CROSS PROTOCOL WITH HYBRID TOPOGRAPHY CONTROL FOR MANETS", Journal of Theoretical and Applied Information Technology, 2017. Vol.95. No.3, ISSN: 19928645.
16. Dr.Srinivasu, N. Entropy based CNN for segmentation of noisy color eye images using color, texture and brightness contour features, International Journal of Recent Technology and Engineering,vol 8,21162124
17. T. Vijay Muni, G Sai Sri Vidya, N Rini Susan, "Dynamic Modeling of Hybrid Power System with MPPT under Fast Varying of Solar Radiation", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 1 (2017), pp.:530-537.
18. M Srikanth, T. Vijay Muni, M Vishnu Vardhan, D Somesh, "Design and Simulation of PV-Wind Hybrid Energy System", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 04-Special Issue, 2018, pp: 999-1005
19. S Ilahi, M Ramaiah, T Vijay Muni, K Naidu, " Study the Performance of Solar PV Array under Partial Shadow using DC- DC Converter", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 04-Special Issue, 2018, pp: 1006-1014.
20. S Moulali, T Vijay Muni, Y Balasubrahmanyam, S Kesav,"A Flying Capacitor Multilevel Topology for PV System with APOD and POD Pulse Width Modulation", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 02-Special Issue, 2018, pp: 96-101.
21. T Vijay Muni, S V N L Lalitha, "Fast Acting MPPT Controller for Solar PV with Energy Management for DC Microgrid", International Journal of Engineering and Advanced Technology (IJEAT), Volume 8, Issue 5, pp-1539-1544.
22. T Vijay Muni, S V N L Lalitha, "Power Management Strategy in Solar PV System with Battery Protection Scheme", International Journal of Innovative Technology and Exploring Engineering, Volume 8, Issue 6, pp-960-964.
23. Dr.Srinivasu, N ,Entropy based CNN for segmentation of noisy color eye images using color, texture and brightness contour features, International Journal of Recent Technology and Engineering
24. Dr.Srinivasu, N Effective segmentation of sclera, iris and pupil in noisy eye images, Telkomnika (Telecommunication Computing Electronics and Control)Volume 17, Issue 5, 2019, Pages 23462354.
25. Dr.K.V.D.Kiran, Hadoop security challenges and its solution using KNOX, Indonesian Journal of Electrical Engineering and Computer Science, Volume 12, Issue 1, 2018, Pages 107116.
26. Dr.K.V.D.Kiran ,A prediction scheme of mobility of cognitive femtocells LTEA / LTEUE under different speed scenarios, International Journal of Engineering and Technology(UAE), Volume 7, Issue 2, 2018, Pages 6467
27. Prakash, K.B. 2018, "Information extraction in current Indian web documents", International Journal of Engineering and Technology (UAE), vol. 7, no. 2, pp. 6871.
28. Prakash, K.B. 2017, "Content extraction studies using total distance algorithm", Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2016, pp. 673.
29. Kolla, B.P. & Raman, A.R. 2019, Data Engineered Content Extraction Studies for Indian Web Pages, Advances in Intelligent Systems and Computing, 711, pp. 505-512.

AUTHORS PROFILE

Dr.K.V.D.Kiran completed his Ph.D CSE from Acharya Nagarjuna University in 2015, and published around 21 scopus indexed journals and having a fellow membership from Innovative Scientific Research Professional and Life Member from CSI, and Received Drona Award from IBM for guiding a project in e-learning concept in 2011 and significant contribution award from CSI in 2015.